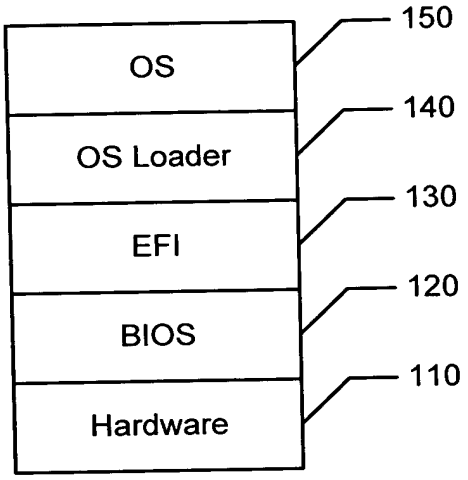
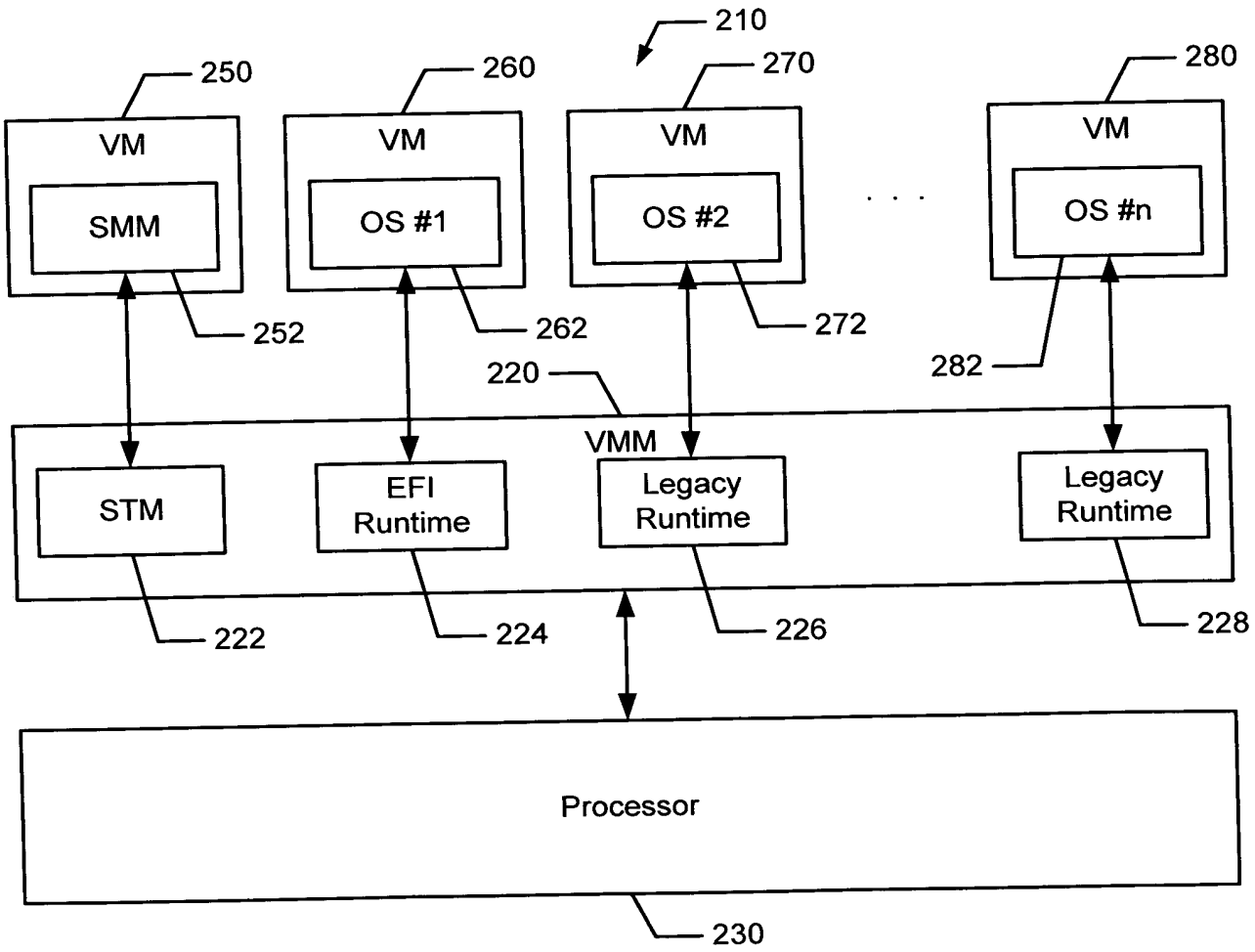


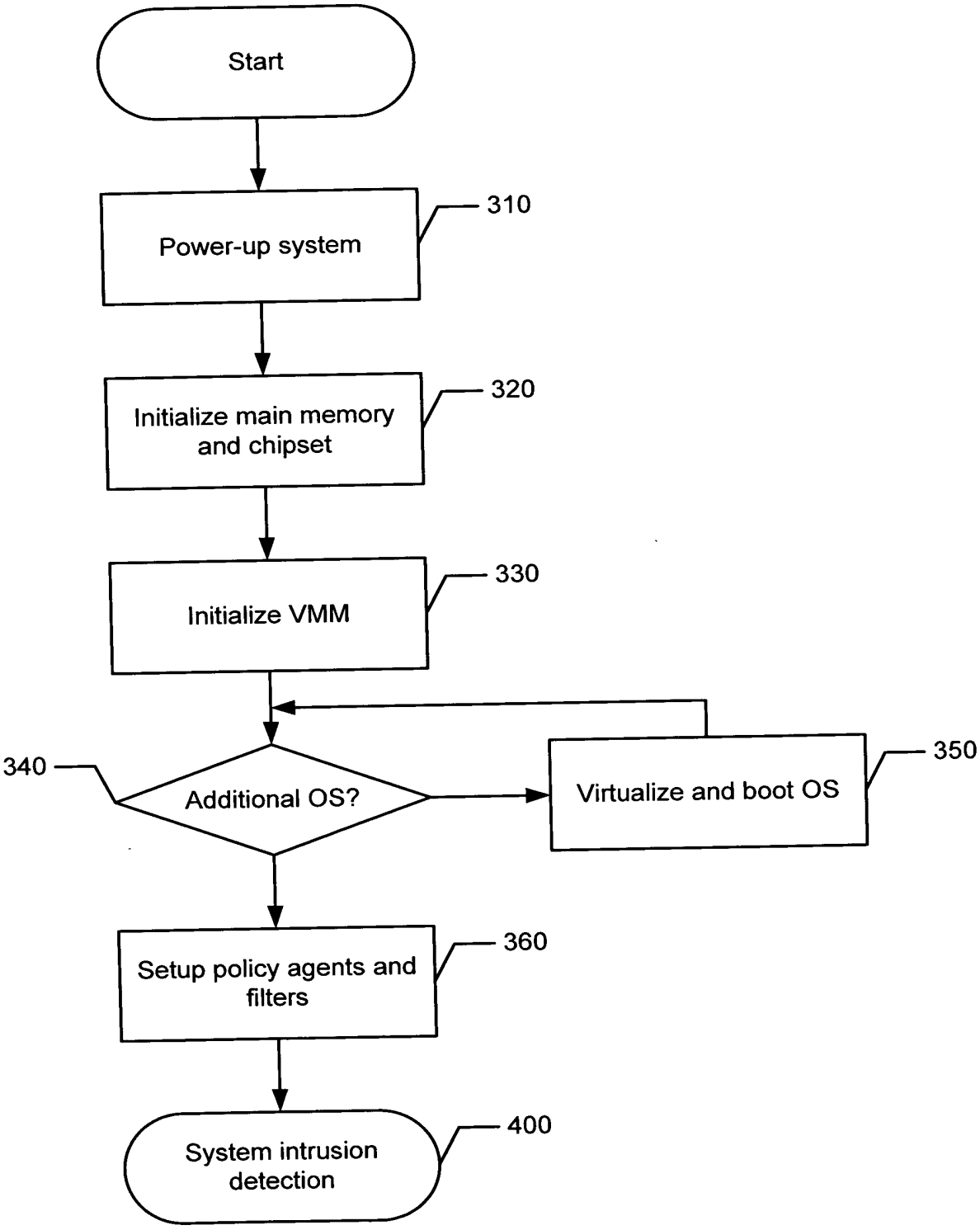
100

FIG. 1



200

FIG. 2


Start
Power-up system
310
Initialize main memory and chipset
320
Initialize VMM
330
340
Additional OS?
Virtualize and boot OS
350
Setup policy agents and filters
360
System intrusion detection
400

300

FIG. 3

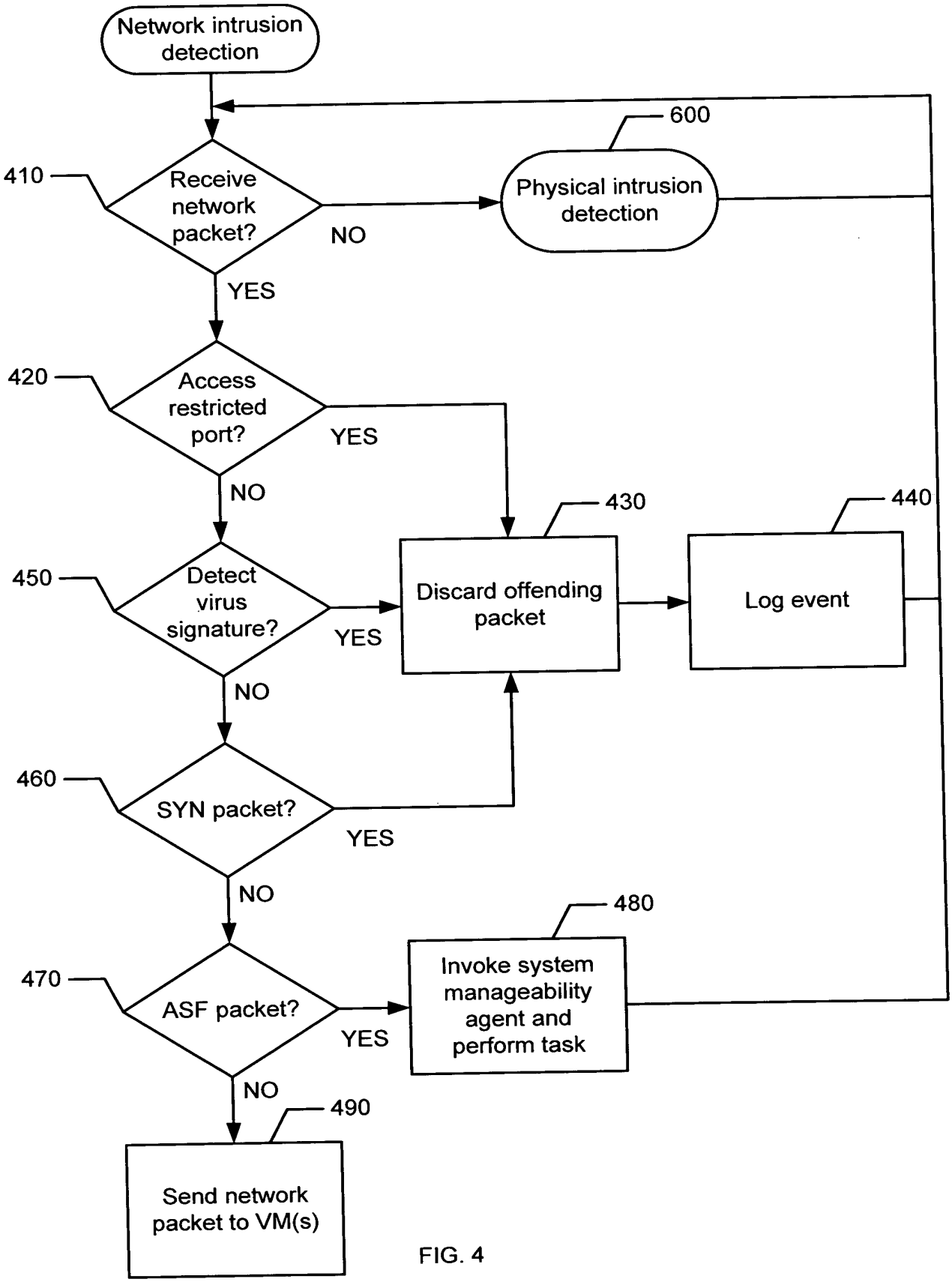
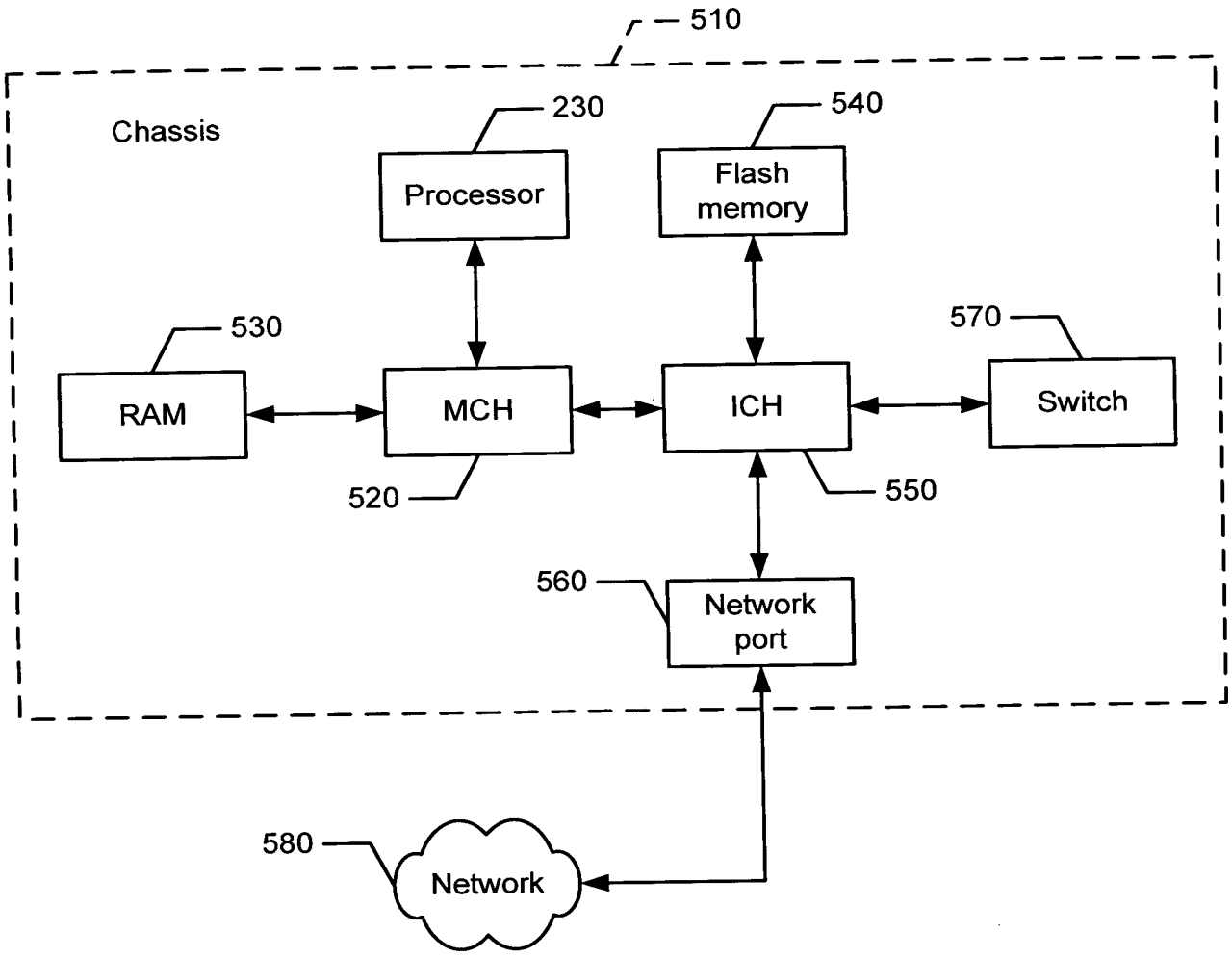

Network intrusion detection
600
410
Receive network packet?
Physical intrusion detection
NO
YES
420
Access restricted port?
YES
NO
430
440
450
Detect virus signature?
Discard offending packet
Log event
YES
NO
460
SYN packet?
YES
NO
480
470
ASF packet?
Invoke system manageability agent and perform task
YES
NO
490
Send network packet to VM(s)

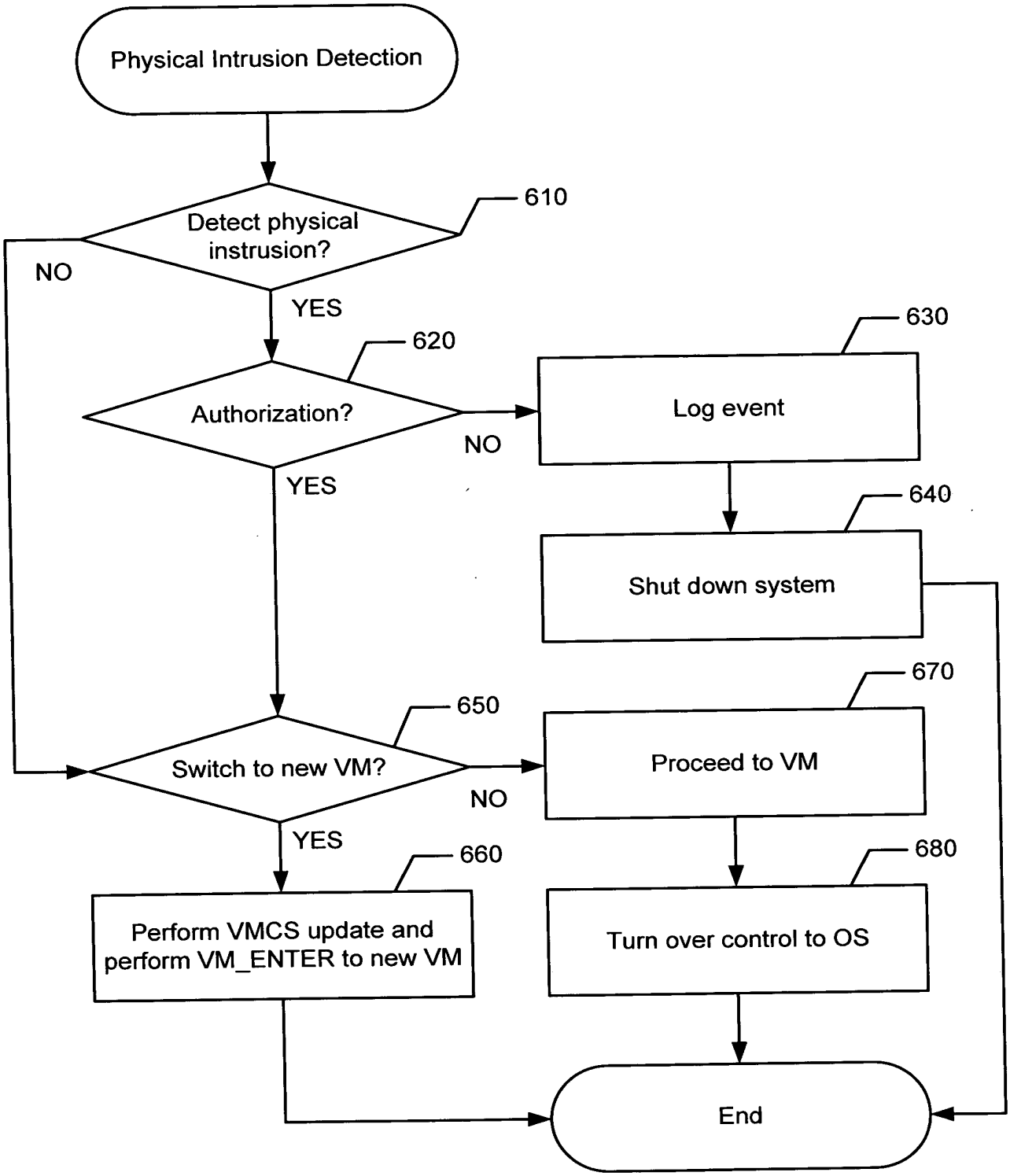
FIG. 4

400


510
Chassis
230
Processor
540
Flash memory
530
RAM
MCH
520
ICH
550
570
Switch
560
Network port
580
Network

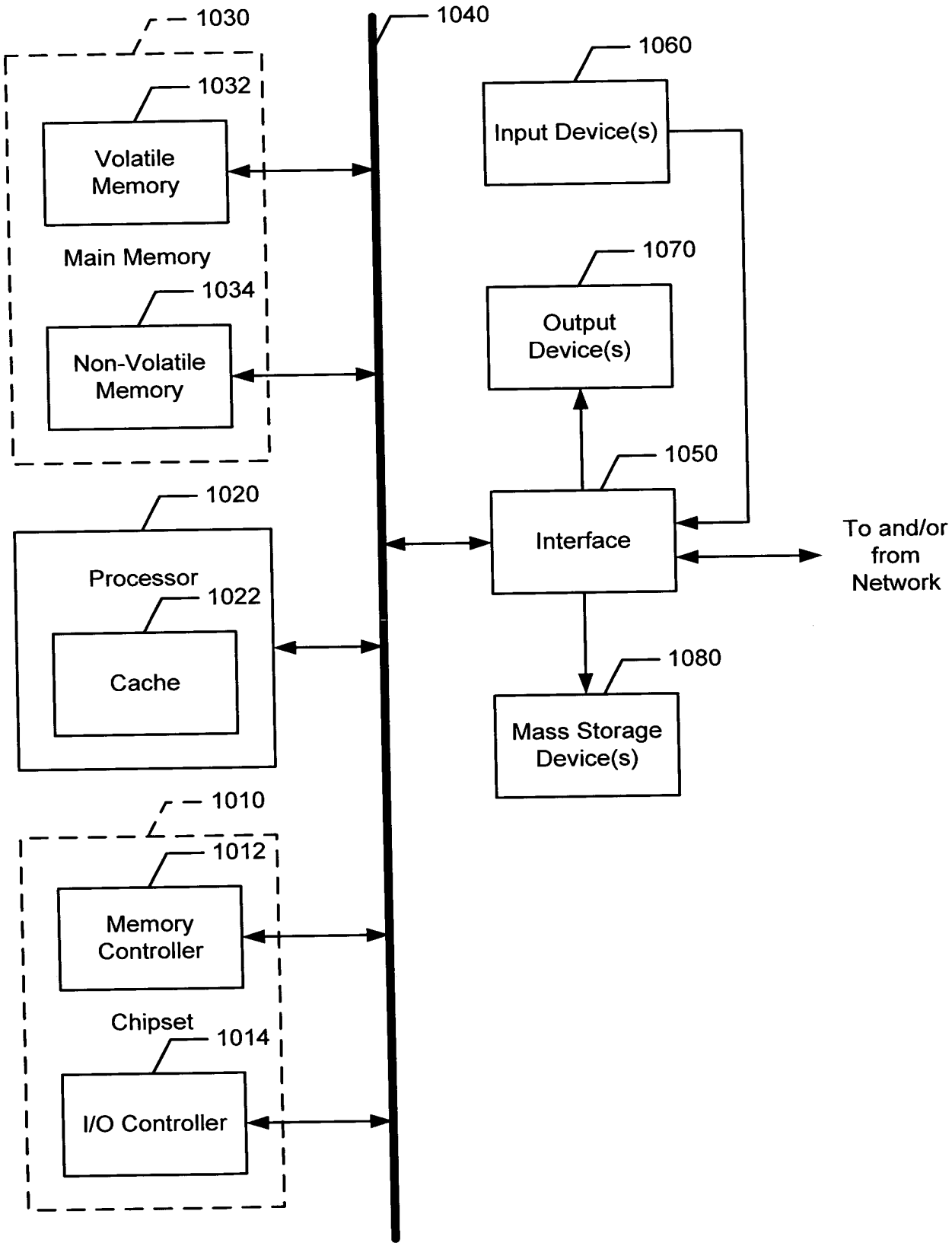
500

FIG. 5


Physical Intrusion Detection
Detect physical instrusion?
610
NO
YES
620
Authorization?
NO
YES
630
Log event
640
Shut down system
650
Switch to new VM?
NO
YES
660
Perform VMCS update and perform VM_ENTER to new VM
670
Proceed to VM
680
Turn over control to OS
End

600

FIG. 6


1030
1040
1060
1032
Volatile Memory
Input Device(s)
Main Memory
1070
1034
Output Device(s)
Non-Volatile Memory
1050
1020
Interface
To and/or from Network
Processor
1022
Cache
1080
Mass Storage Device(s)
1010
1012
Memory Controller
Chipset
1014
I/O Controller

1000

FIG. 7